NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Dike upgrades to slow East Grand Forks traffic. A portion of two important commuter routes in East Grand Forks, Minnesota, Demers Avenue and Bygland Road, will be closed for 2 to 3 weeks due to construction, the Grand Forks Herald reported July 11. The U.S. Army Corps of Engineers is replacing the iron sill plates beneath the street that helps seal the concrete floodwall, according to the East Grand Forks public works director. He said the Corps will remove the sill plates and replace them with concrete because heavy traffic over the area created a hole that could have allowed water to seep in. Source: http://www.grandforksherald.com/event/article/id/240494/

Missile facility scare in North Dakota was a false alarm. The Air Force said an incident at a missile launch facility in northwestern North Dakota that forced the shutdown of a state highway was a false alarm. The military said that July 9, remote sensors incorrectly detected a possible chemical hazard during routine maintenance at the facility from which airmen control missiles buried in underground silos in the countryside. State officials closed Highway 37 south of Parshall during the investigation. The road has since reopened. Source: http://www.wday.com/event/article/id/66096/group/homepage/

Regional

(Minnesota) **Man arrested after allegedly threatening to blow up Charter cable TV building in Duluth.** A Duluth, Minnesota man is in jail pending felony charges of making terroristic threats after allegedly saying he was going to burn or blow up the Charter Communications building in Duluth, then showing up at that facility July 10. He was upset over his Internet service, Duluth police said in a news release. He was being held at the St. Louis County Jail. Police were called to the building after reports of a suspicious vehicle outside the building, according to scanner reports. The incident began when a Charter contact center adviser received a call from a Duluth customer threatening to harm the Duluth office and its employees, said a Charter spokeswoman. Employees in the Duluth office were notified and were evacuated to a safe location, she said. A Charter technical supervisor in Duluth had seen a man in a pickup truck parked in the lot in front of the building, she said. She said the man left the truck before police arrived, but he was apprehended and taken into custody. Source: http://www.duluthnewstribune.com/event/article/id/236513/group/homepage/

(Montana) **Montana ranchers prepare for loss of hay, pastures from fires.** While thousands of cattle and horses were displaced by the wildfires in eastern Montana, stockgrowers on the western side of the State braced for ripple effects to come later the summer of 2012, the Missoula Missoulian reported July 6. The Southeastern Montana Complex of fires burned more than 308,000 acres around Colstrip just as ranchers were putting up their first hay cuttings or starting their seconds. In all, at least 54 major landowners and more than 4,400 cattle lost pasture. Source: http://missoulian.com/news/state-and-regional/wildfires/ranchers-prepare-for-loss-of-hay-pastures-from-fires/article_822814b8-c7ec-11e1-b60d-001a4bcf887a.html

National

Drought stretches across America, threatens crops. A severe drought is spreading across the Midwest, resulting in some of the worst conditions in decades and leaving more than 1,000 counties designated as natural disaster areas, authorities said, CNN reported July 13. Farmers in the region are suffering, with pastures for livestock and fields of crops becoming increasingly parched during June, according to the National Climatic Data Center. Many areas in the southern Midwest are reporting the poorest conditions for June since 1988. As of July 10, about 61 percent of the contiguous United States (excluding Alaska, Hawaii, and Puerto Rico) was experiencing drought, the highest percentage in the 12-year record of the U.S. Drought Monitor. Unusually high temperatures and little rainfall have led to "widespread deterioration and expansion of dryness and drought" in the Midwest, northwestern Ohio Valley, and southern Great Plains, the drought monitor said. That has left 1,016 counties in 26 States termed as natural disaster areas, the U.S. Department of Agriculture said the week of July 9. A county is generally qualified as a natural disaster area if it has suffered severe drought for 8 consecutive weeks. The past 12 months have been the warmest the United States has experienced since records began in 1895, the climatic data center said. Source: http://www.cnn.com/2012/07/13/us/midwest-drought/index.html?hpt=hp_t1

Smart grid's big data opportunities still untapped. North American utilities may be collecting unprecedented amounts of data from millions of new smart meters — 18,000 percent more data, to be exact. That is one finding from a new survey from Oracle released July 10, covering the "big data" challenges and opportunities in the smart grid. The survey of 151 North American utility executives revealed a disconnect between data collection and putting that data to use. For instance, while 78 percent of respondents said their utilities were collecting outage detection data from smart meters, only 59 percent were actually using it for business processes and decision-making as of April 2012, when the survey was conducted. Similar gaps were revealed in voltage data (73 percent collecting it and 57 percent using it), tamper detection data (63 percent collecting it and 47 percent using it), and diagnostic data (56 percent collecting it and only 33 percent using it). Source: http://www.greentechmedia.com/articles/read/smart-grids-big-data-opportunities-still-untapped/

International

Another infiltration reported at South African atomic site. South Africa's Pelindaba nuclear facility in April sustained an unspecified violation of its protective measures, marking the third such case at the site in 7 years, the Johannesburg Times reported July 12. Plant operator South African Nuclear Energy May 7 informed the "relevant" official agency of the incident, which Business Day said happened April 28. South Africa's former apartheid government decades ago conducted nuclear arms research and production at Pelindaba, which now is used to prepare medical isotopes. South African Nuclear Energy and the National Nuclear Regulation both refused to provide details on the recent infiltration or describe protections at the facility. Pelindaba is believed to hold hundreds of pounds of highly enriched uranium, according to the

Washington-based Nuclear Threat Initiative.Source: http://www.nti.org/gsn/article/new-infiltration-reported-south-african-atomic-plant/

Britain's home secretary defends deployment of extra 3,500 Olympic troops. Britain's home secretary defended the handling of Olympic security July 12 after the government said it would deploy another 3,500 troops after a private security firm failed to provide enough guards. The development added to concerns about Britain's preparations for the London Games, which officially open July 27, as fresh problems also emerged with transport and border security. The home secretary made an urgent statement to lawmakers confirming private contractor G4S could not supply all the security staff it promised due to recruitment and training problems. She said the government built in contingency plans to what is Britain's largest security operation since World War II but that "concerns have arisen about the ability of G4S to deliver the required number of guards." The home secretary said she was confident the government would be able to stick to its security budget for the Games. A total of 17,000 troops will now be involved in the Olympics. Source: http://www.google.com/hostednews/afp/article/ALeqM5hnCAH9elDTf9E_EdVB6NgI8Ke2cw?docId=CNG.aa32dcd4159bdbe202be042888a766ee.511

Mexico kills 2.5 mn poultry to contain bird flu. Officials have slain 2.5 million birds at poultry farms in western Mexico over the past 3 weeks to contain a bird flu outbreak, the agriculture ministry said, Agence France-Presse reported July 11. The virus responsible for Mexico's current bird flu outbreak, H7N3, has occasionally caused human disease in various parts of the world, according to the United Nations but has not shown itself to be easily transmittable between humans. Officials said they have visited 148 poultry farms. Of those, bird flu was found in 31 farms, while 34 came up negative, and results for the remainder were pending. Of the 3.4 million affected poultry, "the number of birds that have been sacrificed as a control and eradication measure as of (July 9) is 2.5 million," the ministry said in a statement. The outbreak was first detected June 20 in Jalisco state, and the Mexican government declared a national animal health emergency July 2. After importing 1 million vaccines from Pakistan, farming officials said they have developed a seed-based vaccine that they will deliver to 4 laboratories to produce more than 80 million doses initially. Source: http://www.google.com/hostednews/afp/article/ALeqM5hOw9R4VYbA_zOTbfr3uKSNNrmxUw?docId=CNG.e3bb940ba7cd96953abc2a7998969c09.261

Banking and Finance Industry

Malware now targeting banking applications on Android, says Trusteer. Researchers at Trusteer discovered a type of attack targeting Android users via their desktops, with the aim of controlling both endpoint devices. So far, the malware itself is limited to Spain, Germany, the Netherlands, and Portugal. Trusteer's discovery offers additional insight into the development of SpyEye and Tatanga, the families of malware making headlines recently. This time, Tatanga is combined with elements form SpyEye and used in a scheme to entice users to install an alleged security application. Based on what Trusteer published, it appears that this latest set of attacks is an upgrade and not a new infection point. Once an infected system visits a specialized or pre-

determined domain (often banking related), Tatanga will use Web injects to entice the user to install the security application.Source: http://www.securityweek.com/malware-now-targeting-banking-applications-android-says-trusteer

Chemical and Hazardous Materials Sector

Chemical giant foils infected USB stick espionage bid. An attempt to infiltrate the corporate systems of Dutch chemical company DSM by leaving malware-laden USB sticks in the corporation's car park failed, The Register reported July 11. Instead of plugging the discarded drives into a workstations, which would have infected the company's machines, a worker who first found one of the devices turned it in to DSM's IT department. System administrators subsequently found an unspecified password-stealing keylogger, according to local reports. The spyware was designed to upload stolen usernames and passwords to a server under the control of hackers. This site was blocked by DSM's system administrators, so the firm would be protected even if other workers find and use the infected USBs on corporate laptops. Using infected USBs as way to smuggle malware into firms has become a regular occurrence in recent years, security researchers' note, especially since they were the presumed delivery mechanism of the Stuxnet worm. Source: http://www.theregister.co.uk/2012/07/11/infected_usb_spyware/

Commercial Facilities

Targeted attacks focus on small businesses. Thirty-six percent of all targeted attacks (58 per day) during the last 6 months were directed at businesses with 250 or fewer employees, according to Symantec. During the first half of 2012, the total number of daily targeted attacks continued to increase at a minimum rate of 24 percent with an average of 151 targeted attacks being blocked each day during May and June. Large enterprises consisting of more than 2,500 employees are still receiving the greatest number of attacks, with an average 69 being blocked each day. "There appears to be a direct correlation between the rise in attacks against smaller businesses and a drop in attacks against larger ones. It almost seems attackers are diverting their resources directly from the one group to the other," said a cybersecurity intelligence manager at Symantec. "It may be that your company is not the primary target, but an attacker may use your organization as a stepping-stone to attack another company," he said. The defense industry was the targeted industry of choice in the first half of 2012, with an average of 7.3 attacks per day. The chemical/pharmaceutical and manufacturing sectors maintain the number two and three spots, respectively. These targets clearly received a smaller percentage of overall attention than in 2011, but the chemical/pharmaceutical sector is still hit by one in every five targeted attacks, while manufacturing still accounts for almost 10 percent of all targeted attacks. Source: http://www.net-security.org/secworld.php?id=13225&utm

Communications Sector

AT&T to start blocking stolen cellphones this week. AT&T said it expects to start a program the week of July 9 that will keep track of devices reported stolen, making it more difficult for

thieves to sell the devices on the black market. The company said its database would initially prevent reactivation of stolen devices on its own network. Later in 2012, it plans to expand the database to work with other carriers. In April, the Federal Communications Commission (FCC) said it was working with police departments and wireless carriers to create a database to combat cellphone theft nationwide. Over the last year, one out of three robberies in the United States was related to the theft of a cellphone, the FCC said. Verizon Wireless, the number one carrier in the United States, said that unlike AT&T, it has had its own database for disabling stolen cellphones on its network for years. Verizon will also be participating in the nationwide database when it becomes available later in 2012, said a Verizon spokeswoman. Source: http://bits.blogs.nytimes.com/2012/07/09/att-cellphone-theft/

Sun storms: solar activity at fiery high. The first week of July was an intense period of solar flares, and it showed no signs of stopping, CBS News reported July 9. The week of July 2 saw several huge solar flares, the biggest of which occurred July 6. Labeled an X1.1 class solar flare — the strongest classification used by the U.S. Space Weather Prediction Center — the sun storm caused radio blackouts on Earth as particles ejected from the sun crashed into the planet's atmosphere. It was the fifth X-class solar flare of 2012. Earlier the week of July 2, several other powerful solar flares erupted from the sun. Most of them appear to be coming from the same area, a giant sunspot called AR1515. Technically a group of sunspots, AR1515 is an enormous plain of volatile activity. Source: http://www.cbsnews.com/8301-205_162-57468785/sun-storms-solar-activity-at-fiery-high/

Critical Manufacturing

Nikon recalls rechargeable battery packs sold with digital SLR cameras due to burn hazard. The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with Nikon Inc., July 11 announced a voluntary recall of the about 201,100 EN-EL 15 digital SLR camera battery packs. The battery packs can short circuit, causing them to overheat and melt, posing a burn hazard to consumers. Nikon has received seven reports of incidents of the recalled battery packs overheating. The battery packs were sold at camera, office supply, and mass merchandise stores, in catalogs and on various Web sites nationwide, and with the Nikon digital SLR D800 and D7000 model cameras. Consumers should stop using the recalled battery packs immediately, remove them from the camera, and contact Nikon for a free replacement battery pack. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12219.html

Family Dollar stores recalls decorative light sets due to fire and electrical shock hazard. The U.S. Consumer Product Safety Commission, in cooperation with Family Dollar Services Inc., July 12 announced a voluntary recall of about 280,000 mini lights. The light sets do not meet standards for this product and pose a fire and shock risk. There were three reports of overheating. The lights were sold at Family Dollar stores from September 2011 through December 2011. Consumers should immediately stop using the light sets and return the products to Family Dollar stores for full refunds. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12222.html

Bosch recalls SkilSaw miter saws due to laceration hazard. The U.S. Consumer Product Safety Commission, in cooperation with Robert Bosch Tool Corporation of Mount Prospect, Illinois, July 10 announced a voluntary recall of approximately 22,149 miter saws. Consumers should stop using recalled products immediately unless otherwise instructed. The lower guard can break and contact the blade during use, posing a laceration hazard. The miter saws were sold at Lowe's Home Centers nationwide, and OC Tanner from January 2012 to April 2012. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12218.html

NHTSA recall notice - Isuzu Amigo and Rodeo Sport suspension corrosion. Isuzu announced the recall of 11,221 model year 1998-2000 Amigo and model year 2001-2002 Rodeo Sport vehicles July 7. The vehicles may experience excessive corrosion in the vicinity of the forward mounting point bracket for the left or right rear suspension link. Excessive corrosion may result in the left or right rear suspension lower link bracket becoming detached from the frame, which can affect vehicle handling and increase the risk of a crash. Dealers will inspect the rear suspension. For vehicles in which little or no corrosion is found, the area will be treated with an anti-corrosive compound. For vehicles in which corrosion has damaged the rear suspension lower link bracket and affected its connection to the vehicle frame, a reinforcement bracket will be installed. In the rare event of severe corrosion, Isuzu will offer to repurchase the vehicle for an amount based on the Kelly Blue Book price. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V306000&summary=true&prod_id=203822&PrintVersion=YES

Defense/ Industry Base Sector

More F-22 scares prompt new calls for action. Two more pilots were forced to land F-22s in recent weeks after experiencing symptoms of oxygen deficiency, two lawmakers said July 10. The incidents led a Republican Representative from Illinois and and a Democratic Senator from Virginia to renew calls to the U.S. Air Force to pinpoint the cause of problems that have plagued the service's stealth fighter for 2 years. July 6, an F-22 pilot at Joint Base Pearl Harbor-Hickam in Hawaii declared an emergency and landed safely, just weeks after a similar incident at Joint Base Langley-Eustis in Virginia, the lawmakers said. Both pilots were flying without pressurized vests, the lawmakers said. The pressurized vests emerged as a possible cause of the problems in early June, though the director of operations for Air Combat Command said then that the Air Force was not ready to declare victory. Pilots were directed, in most cases, to fly without the vest. The Congressmen sent a letter to the Air Force Secretary July 10, outlining their concerns and asking for additional updates into the service's investigation. The letter requests an update within 30 days on all F-22 incidents, and requests more data on the investigation into the pressurized vests. The lawmakers also want details on a recent contract awarded to Lockheed Martin for the installation of an automatic backup oxygen supply system. The Air Force plans to install the system in F-22s later in 2012. Source: http://www.militarytimes.com/news/2012/07/air-force-f-22-raptor-scares-new-calls-for-action-071012/

Emergency Services

No parts available for C-130 wildfire tankers. The demise of the only company that manufactured a device specially designed to spray fire retardant from the back of U.S. military C-130 cargo planes has some experts worried about the future viability of a program that has helped fight wildfires for 40 years, the Associated Press reported July 7. The Modular Airborne Firefighting System is a bus-sized device that can be shoved into the belly of a cargo plane and used to spray retardant, or slurry, at 3,000 gallons in less than 5 seconds. The $4.9 million device's only manufacturer, Sacramento, California-based Aero Union, went out of business in August 2011, and no other company has replaced it. Critical spare parts also are no longer being made. The MAFFS C-130s are operated by three National Guard units and one Air Force Reserve unit in Wyoming, Colorado, North Carolina, and California. Wyoming's MAFFS have been deployed as far away as Indonesia. In 2011, MAFFS C-130s flew to wildfires in Arizona, New Mexico, Texas, Oregon, and Mexico. Source: http://www.militarytimes.com/news/2012/07/ap-air-force-no-parts-for-c-130-wildfire-tankers-070712/

(West Virginia) **Metro 911 Center down following lightning strike.** The Ned Chilton Metro 911 Center in Charleston, West Virginia, was struck by lightning July 5 — an event that forced officials to reroute calls to the Kanawha County Emergency Ambulance Authority (KCEAA). The building sustained a direct hit when a strong storm moved through the area, the county manager said. The strike knocked out telephone lines and radio communications with emergency responders. Officials called the KCEAA on cell phones, instructing workers there to begin taking 9-1-1 calls, she said. Dispatchers were also sent to the authority's offices to help take calls. Officials at the 9-1-1 center were still assessing the damage. Frontier Communications personnel were there July 5 trying to get the phones working again. Officials found some computer consoles were damaged, the commission president said. One of the emergency generators also sustained some damage, he said. Source: http://www.dailymail.com/News/Kanawha/201207050108

Energy

(Pennsylvania) **Protesters lead to temporary shutdown of Pa. rig.** An energy company said protesters demonstrating against hydraulic fracturing at a Pennsylvania State forest led to a gas drilling rig temporarily being shut down. An EQT Corp. spokeswoman said the company shut down the rig in Moshannon State Forest July 8. She said the Pittsburgh-based company's primary concern is the safety of its employees and contractors. Police were at the site trying to maintain order. A spokeswoman with Marcellus Protest said 150 protesters blocked an access road for trucks headed to the EQT rig. Source: http://www.abc27.com/story/18975681/protesters-lead-to-temporary-shutdown-of-pa-rig

Food and Agriculture

U.S. corn-crop forecast cut as drought dims supply outlook. The United States cut its corn-harvest estimate 12 percent and said inventories in 2013 will be smaller than forecast in June as

the worst Midwest drought since 1988 erodes prospects for a record crop. Farmers will harvest 12.97 billion bushels, down from a June prediction of 14.79 billion, the U.S. Department of Agriculture (USDA) said July 11 in a report. Analysts expected 13.534 billion, based on the average of 14 estimates in a Bloomberg survey. Inventories before the 2013 harvest may be 1.183 billion bushels, down 37 percent from 1.881 billion forecast in June, the USDA said. Source: http://www.businessweek.com/news/2012-07-11/u-dot-s-dot-corn-crop-forecast-cut-as-drought-dims-supply-outlook

Environmental changes lead stressed cows in southern U.S. to produce less milk. "Cows are happy in parts of Northern California and not in Florida" is a good way to sum up the findings of new research from the University of Washington, said one of the report's authors, Homeland Security News Wire reported July 12. A University of Washington release reports the study combined high-resolution climate data and county-level dairy industry data with a method for figuring out how weather affects milk production. The result is a more detailed report than previous studies and includes a county-by-county assessment — that will be available to farmers — of the impact climate change will have on Holstein milk production in the United States through 2080. Previous research into how climate affects cow milk production in the United States was either limited in geographic scope or was too simplistic, ignoring the impact of humidity, for instance. By using detailed climate data covering night and day across the entire country, however, the researchers made some new discoveries. For instance, in Tillamook, Oregon, where the climate is humid and the nighttime temperature does not change much, milk production begins to drop at a much lower temperature than in the dry Arizona climate. Source: http://www.homelandsecuritynewswire.com/dr20120712-environmental-changes-lead-stressed-cows-in-southern-u-s-to-produce-less-milk

Federal Egg Safety Rule goes into full effect. The government's Egg Safety Rule, a set of requirements designed to prevent Salmonella contamination at laying facilities, became fully fledged July 9 when it went into effect for medium-sized operations after previously applying only to large producers. Since July 2010, companies with over 50,000 laying hens have been required to comply, but the rule now covers facilities with more than 3,000 and less than 50,000 hens. The rule requires all producers who do not pasteurize in-shell egg products to test for Salmonella Enteriditis bacteria and to refrigerate eggs at 45 degrees or less during storage and transportation, starting within 36 hours of when they are laid. It also says chicks and young hens may only be sourced from suppliers who monitor for Salmonella. Firms must implement biosecurity, rodent, and pest control measures. The rule says that if Salmonella is found on eggs or in a laying facility, the eggs must be pasteurized or diverted for non-food use, and the facility must be sanitized. Source: http://www.foodsafetynews.com/2012/07/egg-safety-rule-now-in-full-force/

New Jersey firm recalls various frozen, ready-to-eat meat and poultry products due to potential Listeria monocytogenes contamination. Buona Vita, Inc., a Bridgeton, New Jersey establishment, recalled approximately 324,770 pounds of various frozen, ready-to-eat meat and poultry products due to possible contamination with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced July 7. The

products were sold to distribution facilities nationwide. The problem was discovered through microbiological testing by the FSIS and the Ohio Department of Agriculture. Source: http://www.fsis.usda.gov/News_&_Events/Recall_042_2012_Release/index.asp

(Indiana) **Drought season highlights damage caused by nematodes.** The drought throughout Indiana was intensifying nematode damage in farm fields, said a Purdue Extension nematologist, AgAnswers reported July 5. The needle nematode, soybean cyst nematode, and lance nematode all were causing more problems for grain farmers in a year when crops already are stressed by extreme heat and lack of rain. The nematologist said nematodes, microscopic roundworms, can be found in fields every year, but the damage is worse during a drought season. The needle nematode exclusively feeds on corn and grasses and is found in sandy soils. The lance nematode is found in corn and soybean fields. The soybean cyst nematode attacks soybean plants and causes the plant to become yellow and stunted. Source: http://www.agprofessional.com/news/Drought-season-highlights-damage-caused-by-nematodes-161426105.html

Government Sector (including Schools and Universities)

Threats lurk among Pentagon's sprawling computer networks. To heighten security and lower costs, the Defense Department is attempting to build a "joint information environment" that would simplify military computing, officials July 10 told military personnel at a talk sponsored by Government Executive Media Group. The goal by 2017 is to consolidate information technology contracts across services, move off desktops to online services accessible from any device, and create what Cyber Command calls a "cyber operational picture." The existing intrusion prevention system "is not providing that real-time information that we need," the director of C4 Systems and Cyber Command chief information officer said during an interview after the event. A comprehensive snapshot of anomalous network activities and instant Defense-wide access to threat information from softer targets, such as utilities, could reveal a potential coordinated attack, he said. The Host-Based Security System is a starting point for reaching this wide-angle view, he said. The system is deployed throughout the military services and agencies but is not fully operational "with all the modules enabled." The statistics collected from many of the Defense organizations must be manually combined, he added. Source: http://www.nextgov.com/cybersecurity/2012/07/threats-lurk-among-pentagons-sprawling-computer-networks/56700/

(Virginia; Washington, D.C.) **Mass. man to plead in plot to blow up Pentagon.** A Massachusetts man charged with plotting to fly remote-controlled model planes packed with explosives into the Pentagon and U.S. Capitol in the Washington-D.C. area plans to plead guilty to two charges, his lawyers and prosecutors said in a plea agreement filed in federal court July 10. He was arrested in September 2011 after federal employees posing as al Qa'ida members delivered materials he had allegedly requested, including grenades, machine guns, and what he believed was 24 pounds of C4 explosives. In the plea agreement, prosecutors and his lawyers say he will

plead guilty to attempting to provide material support to terrorists and attempting to damage and destroy federal buildings by means of an explosive. Prosecutors and defense attorneys agreed to request a 17-year sentence. Source: http://www.militarytimes.com/news/2012/07/ap-military-pentagon-plot-massachusetts-man-to-plead-guilty-071012/

(Washington) **Explosives found at 2 Kent schools, 1 school damaged by blast.** Over the course of 48 hours, two separate explosive devices were found at two different schools in Kent, Washington, KCPQ 13 Seattle reported July 6. The first device detonated and blew a hole in the wall of Lake Youngs Elementary School. The explosion sent rubble from the wall about 100 feet from where the device was detonated. Kent fire officials said someone broke a window at the school and climbed inside, then set off the explosive. "It actually blew a very large hole about 6 feet high and 2 feet wide in a masonry wall," said a Kent Fire Department official. "Somebody could have been seriously hurt in that one." He said the device could have been a high-powered commercial firework or a powerful "improvised explosive device." Investigators with the Bureau of Alcohol, Tobacco, Firearms and Explosives are helping in the investigation. The second incident happened July 5 at Glenridge Elementary School where an unexploded "sparkler bomb" was found by a police officer in the parking lot. Fire investigators confirmed the device was dangerous and if it had detonated, it could have injured someone. Source: http://www.q13fox.com/news/kcpq-explosives-found-at-2-kent-schools-1-school-damaged-by-blast-20120706,0,6495446.story

(Pennsylvania) **Officials complete sweep of Pennsylvania Capitol building after false bomb threat.** The Pennsylvania State Capitol building in Harrisburg was evacuated July 6 because of a reported bomb threat, according to a State Department of General Services spokesman. The report turned out to be a false bomb threat. He said it was the first bomb threat to the Main Capitol building in years. The call came in to State Police and they determined it to be a credible bomb threat, the spokesman said. The caller said an explosive device was in the building and it would detonate within 2 hours. Instead of sounding an alarm, the spokesman said the decision was made to use the employee notification system to individually ask people to leave the building and not plan on returning that evening. He said the decision was made given the low-occupancy of the Capitol at that time of day during a holiday week. "If we had evacuated the building, we'd have everybody standing out in the heat with no access to their cars for possibly 3 hours," he said. The bomb sweep was completed later that evening. Source: http://www.pennlive.com/midstate/index.ssf/2012/07/pennsylvania_capitol_building_1.html

(Georgia) **Atlanta City Hall evacuated after bomb scare.** The Atlanta City Hall was evacuated July 6, and a police bomb squad was called in to investigate a suspicious package in a courtyard of the government complex. The package was a backpack tied to a tree, according to a police spokesman. "After detonating the package, it was determined to contain toiletries and clothing," he said. The spokesman said all streets within a two-block radius of city hall were closed, but they were reopened. Source: http://www.ajc.com/news/atlanta/atlanta-city-hall-evacuated-1473021.html

(New Jersey) **Thieves take advantage of storm by stealing from victims in Salem County.** Thieves took advantage of a storm the weekend of June 30 by stealing from its victims in Salem County, New Jersey, authorities said July 5. The storm swept through the county early June 30 ripping down trees and power lines and leaving thousands without power. According to police, two large, industrial-size generators were stolen from a Comcast location July 1. The same day, police received reports that some people were involved in trying to steal downed utility cable. According to police, the individuals were supposedly cutting the downed wire and coiling it up, apparently hoping to sell it for scrap. Police added that it was dangerous because wires could still be live. Source: http://www.nj.com/sunbeam-news/index.ssf/2012/07/thieves_take_advantage_of_stor.html

(Maine) **Three homemade bombs explode in Winslow.** The State of Maine's Fire Marshal's Office is investigating 3 consecutive days of small fires involving homemade fire bombs in Winslow, Maine, the week of July 2. Police roped off a parking lot July 5 at Winslow Junior High School so investigators could comb the scene of the latest incident. The device was made from an aerosol can and a carbon-dioxide canister, said a supervisor with the State Fire Marshal's Office. "We're trying to figure out what it is," he said. "The components and the way they're constructed are a little unconventional. It is something we have to work at." The investigator said two other devices had burned in Winslow in recent days at street corners. The fire supervisor said the three incidents, which took place within 2,000 feet of each other, could be related.Source: http://www.pressherald.com/news/Fire-bomb-blazes-in-Winslow-under-investigation.html

Information Technology and Telecommunications

Yahoo! confirms data breach. Yahoo! confirmed approximately 450,000 e-mail addresses and passwords from its log-in system were leaked on the Internet. The breach was publicized after a security expert posted about it on Twitter and was initially believed only to concern the Yahoo! Voice service. According to Yahoo!, an "old file" from the Yahoo! Contributor Network content sharing platform was compromised and is the source of the log-in data. The company said only around 5 percent of the leaked 450,000 e-mail address and password combinations have valid passwords. Yahoo! stated it is working on fixing the vulnerability and will change the passwords of affected users as well as notify other companies whose user accounts were affected by the breach. In addition to the 140,000 Yahoo! e-mail addresses, there were over 100,000 Gmail addresses and many from Hotmail and other services. Source: http://www.h-online.com/security/news/item/Yahoo-confirms-data-breach-1640148.html

Facebook launches malware checkpoints for users with infected computers. July 10, Facebook launched a feature that allows users to lock down their Facebook accounts and perform malware scans if they suspect their computers might be infected. Facebook already uses internal scanners to detect spam and malicious messages that might have been sent from user accounts hijacked by malware. When found, such accounts are temporarily locked down and their owners are asked to go through a multi-step account recovery process that involves downloading and running a malware scanner called McAfee Scan and Repair. The new

"malware checkpoints" feature will allow users who believe their computers might be infected to initiate the account lockdown procedure themselves and perform an antivirus scan for free. Users will be able to choose to scan their computers with McAfee Scan and Repair, a run-once anti-malware scanner, or with Microsoft Security Essentials, a full-featured antivirus product that must be downloaded and installed. Source: http://www.computerworld.com/s/article/9229005/Facebook_launches_malware_checkpoints_for_users_with_infected_computers

Hackers could target Chrome users' webcams, security experts warn. Google announced a beta version of its Chrome Web browser in a blog post July 10, but experts warned of security threats it might cause for users. The Chrome Beta release grants Web applications access to users' Web cams and microphones without a plugin through the Getusermedia application programming interface (API) — a method that allows users to interact with HTML5 applications through video and audio devices. However, the director of security research and communication at Trend Micro warned that Getusermedia will be attractive to criminals. Source: http://www.theinquirer.net/inquirer/news/2190523/hackers-target-chrome-users-webcams-security-experts-warn

Mobile ads can hijack your phone and steal your contacts. Tens of thousands of smart-phone applications are running ads from rogue advertising networks that change smart-phone settings and take contact information without permission, according to a new study released July 9. Aggressive ad networks can disguise ads as text message notifications or app icons, and sometimes change browser settings and bookmarks. Often, the ads will upload your contacts list to the ad network's servers — information the ad network can then sell to marketers. As many as 5 percent of free mobile apps use an "aggressive" ad network to make money, according to Lookout, a San Francisco-based mobile security company. With millions of mobile apps in stores, that small percentage adds up to a big number. The study found that 19,200 of the 384,000 apps it tested used malicious ad networks. Those apps were downloaded 80 million times. Source: http://www.dailyfinance.com/2012/07/10/mobile-ads-can-hijack-your-phone-and-steal-your-contacts/

ICS-CERT warns of malware that spreads via USB drives. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned organizations to be cautious when handling removable media flash drives since there are many malicious elements that use them to spread. They cite an incident that took place in April 2012. Workers in an energy company identified a piece of malware on a USB stick left by mistake in the USB port of a human-machine interface (HMI) computer by another staffer. The Hamweq virus was not able to perform its tasks because it depended on the operating system's auto-run function, which was disabled on all devices. If the auto-run feature was enabled, the threat could have injected malicious code and created a backdoor that may have been leveraged by the attackers to steal sensitive data. According to ICS-CERT, in order to avoid similar incidents, organizations should always properly mark removable media. They should also disable auto-run functions when possible. Other recommendations include the use of dedicated media for the same type of systems, and the separation of malfunctioning or potentially infected drives from ones cataloged as acceptable.

The workers that operate industrial control systems should never connect removable media drives with an unknown origin to a system without properly checking first. They should also avoid using personally owned devices for work-related tasks. Source: http://news.softpedia.com/news/ICS-CERT-Warns-of-Malware-that-Spreads-Via-USB-Drives-280442.shtml

Hackers steal BMWs in 3 minutes using security loophole. There has been an unusual spike in the number of BMWs stolen in the United Kingdom, and the method suspected involves devices that plug into the car's OBD port to program blank key fobs, Jalopnik reported July 8. The essential theft process varies in detail, but all reports seem to have a fundamental methodology in common. First, the car is entered, either via nearby RF jammers that block the fob lock signal from reaching the car or by breaking a window. In cases of the window break, the thieves seem to be exploiting a gap in the car's internal ultrasonic sensor system to avoid tripping the alarm. Once access to the vehicle is gained, the thieves connect a device to the car's OBD-II connector which gives them access to the car's unique key fob digital ID, allowing them to program a blank key fob on the spot. BMW is not the only car company to allow key code access through the OBD port, but the recent rash of BMW thefts, compared to other makes, suggests another factor may be at play, possibly a good supply of blank BMW key fobs. Source: http://www.technolog.msnbc.msn.com/technology/technolog/hackers-steal-bmws-3-minutes-using-security-loophole-868400

Warning: Fake Skype app on Android is malware. Cybercriminals created a fake version of the Skype for Android application, designed to earn money from unsuspecting users. Trend Micro, which first discovered the malware, is calling this particular threat JAVA_SMSSEND.AB. The app only runs on older (pre Software Installation Script) Symbian phones or Android devices that allow execution of Java MIDlet. The cybercriminals behind this scheme set up fake Web sites advertising fake Skype apps. Most of the sites are hosted on Russian domains (.ru) but the fake apps themselves are hosted on Nigerien domains (.ne). Source: http://www.zdnet.com/warning-fake-skype-app-on-android-is-malware-7000000418/

Olympic officials brace for hackers competition. Since 2008, U.K. officials said the country was expecting an unprecedented level of attacks during the 2-plus weeks of the 2012 Summer Olympics. The CTO of Cigital said he thought the worst that could happen was hacktivism. However, there are also bigger threats, a retired military intelligence officer and information operations expert and consultant said. "There are a ton of other things, such as schedules, transportation systems, water, physical security, telephones — you name it — all automated and networked. Those would be great targets and shutting down all the water would shut down the Olympics." The competition between the white and black hats is expected to be fierce. Atos, the lead technology company for the summer and winter Games since 2002, will be in charge of about 11,500 computers and servers across the United Kingdom. Atos has done more than 200,000 hours of testing, including mounting simulated attacks, according to the company's executive vice president. Source: http://www.pcworld.com/businesscenter/article/258852/olympic_officials_brace_for_hackers_competition.html

New Android trojan infects 100,000 in China. A new Android trojan that provides a variation on covert premium calls was located in China: it secretly buys applications via China Mobile's Android Market. The cost is automatically added to the user's phone bill. Security firm TrustGo Mobile discovered the malware the week of July 2, and called it Trojan!MMarketPay.A@Android. The malware was found in 9 China app markets and has already infected more than 100,000 Android devices. TrustGo warns the trojan may be delivered as a repackaged app, such as cn.itkt.travelskygo or com.funinhand.weibo. Currently, TrustGo concludes "this sophisticated new malware could cause unexpected high phone bills." The same methodology could also be used to download and install "free" spyware or spyware-infected apps that might have been planted in the Market. Source: http://www.infosecurity-magazine.com/view/26859/

Android malware pandemic set to intensify through 2012. The number of cyber attacks targeting Android mobile devices is far higher than initially predicted, according to security firm Trend Micro. The company reported detecting 25,000 Android malware samples in the second quarter of 2012, more than double the 11,000 it predicted for the period, and 4 times greater than the 6,000 found in the first quarter. Trend Micro predicted the boom seen so far will accelerate further as the year progresses. It estimates there will be around 38,000 malicious samples in the third quarter of 2012, and 129,000 in the fourth quarter. Trend also reported 17 malicious apps were downloaded more than 700,000 times from the Google Play store. Two of these included fake versions of popular sports game apps, suggesting the firm's Bouncer tool is proving inadequate at detecting numerous rogue applications. Source: http://www.v3.co.uk/v3-uk/news/2189268/android-malware-pandemic-set-intensify-2012

Google says spam not coming from Android botnets. July 5, Google dismissed the possibility that a new wave of pharmacy, penny stock, and e-card spam e-mails were being sent by Android spam botnets. "Our analysis suggests that spammers are using infected computers and a fake mobile signature to try to bypass anti-spam mechanisms in the email platform they're using," a Google spokesman said in response to security researchers from Microsoft and antivirus firm Sophos who first identified what they believed to be the work of an Android botnet. The researchers do not have a copy of the Android malware responsible for this spam campaign, but there is indirect evidence that suggests the e-mails are being sent from Android devices. Not all security researchers are convinced by the evidence found so far. Source: http://www.computerworld.com/s/article/9228826/Google_says_spam_not_coming_from_Android_botnets

National Monuments and Icons

(Idaho; Colorado; Utah) **Firefighters battle large blaze in southern Idaho.** Efforts to contain a large wildfire in southern Idaho by July 8 were dashed as winds picked up and the region's grass and sagebrush provided readily available fuel for a blaze estimated at 117 square miles. The fast-moving fire west of Twin Falls, Idaho, was first spotted July 7 and grew to 75,000 acres within 24 hours. The wildfire initially threatened a handful of homes near the hamlet of

Roseworth, 25 miles southwest of Twin Falls, but winds shifted and moved the blaze north. By July 8, no structures were being threatened by the fire, which was 20 percent contained. Recent widespread rainfall allowed crews to gain the upper hand on several fires in Colorado, including the two most destructive in State history. The High Park Fire near Fort Collins was under control, while the Waldo Canyon Fire in Colorado Springs was 98 percent contained. In Utah, cooler temperatures and rain helped firefighters make progress on the State's largest active blaze. The 108,132-acre Clay Springs Fire — burning in steep, rocky terrain in Millard and Juab counties — was 85 percent contained July 8. In Kane County, the human-caused, 8,200-acre Shingle Fire was 50 percent contained. Evacuation orders remained in effect for Stout Canyon subdivisions and portions of two subdivisions south of Highway 14. In Carbon County, the lightning-caused 48,397-acre Seeley Fire near Huntington was 47 percent contained July 8. Source: http://www.sltrib.com/sltrib/world/54452252-68/fire-contained-sunday-percent.html.csp

(Washington, D.C.) **Earthquake-damaged Washington Monument may be closed into 2014.** The earthquake-damaged Washington Monument in Washington, D.C., could remain closed into 2014, the National Park Service said. Its repairs will require the exterior and part of the interior of the 555-foot structure to be shrouded in scaffolding, the Washington Post reported July 9. The estimated $15 million project could require the temporary removal of part of the granite plaza surrounding the monument, and involve construction of an access road on the south side of its grounds. The superintendent of the Park Service's National Mall and Memorial Parks said the project also may require the temporary removal of some of the plaza's flagpoles and benches. The marble and granite monument was extensively damaged by the 5.8 magnitude earthquake that struck the area August 23, 2011. The structure — especially near the top — sustained cracks and loosened pieces of stone and lost mortar. The monument has been closed since. Repairs should be underway by fall 2012. Source: http://www.washingtonpost.com/local/earthquake-damaged-washington-monument-may-be-closed-into-2014/2012/07/09/gJQAXrTNYW_story.html

Western wildfire crews helped by moderating weather. Firefighters around the western side of the United States took advantage of moderating conditions to make inroads against wildfires that destroyed homes, forced residents to evacuate, and burned hundreds of thousands of acres of timber and brush. However, a new wildfire near Redding, California, was causing problems July 6, just hours after it was spotted and quickly grew to 1,200 acres. Authorities said the fire was threatening dozens of homes and forced evacuations. In Colorado, crews expected to fully contain the State's most destructive wildfire July 6. Colorado Springs officials lifted evacuation orders for 126 more homes at the 28-square-mile Waldo Canyon fire, which damaged or destroyed nearly 350 homes and killed 2 people. Authorities said July 5 that they know where the fire started but did not disclose the location. In Wyoming and Montana July 5, firefighters took advantage of a lull in heat and shifting winds to attack wildfires. In southeastern Montana, more than 1,300 personnel took advantage of calm winds and temperatures in the 80s to make headway on five fires that officials were managing as one 480-square-mile wildfire complex so they could quickly deploy resources among the fires. In Utah, rain and cooler temperatures helped crews hold fire lines on the 8,200-acre Shingle fire. The

fire threatened 550 cabins and summer homes in Dixie National Forest. Source: http://www.huffingtonpost.com/2012/07/06/western-wildfires-2012-weather_n_1653353.html

Postal and Shipping

(Texas) **Local mailbox target of thieves 'phishing' scam.** Residents in Fort Worth, Texas, notified the U.S. Postal Service (USPS) July 12 of what appeared to be a phishing scam set up at a neighborhood mailbox. The scam is an example of a crime that, according to the local postal inspector, has resulted in 30 arrests across the metroplex since October 2011. Someone coated the internals of a large, blue stand-alone neighborhood mailbox with an adhesive. A man who lives in a home nearby called the USPS after realizing mail would stick to the surface as it was dropped into the box. The local postal inspector said it is a crime that surfaces occasionally, with thieves looking for money or identity information. The most common tactic they said was to push something sticky into the box in an attempt to grab mail and pull it back out. The postal service has trained mail carriers to look for the adhesive and report it. The mailbox that had been tampered with had been cleaned by the evening. Source: http://dfw.cbslocal.com/2012/07/13/local-mailbox-target-of-thieves-phishing-scam/

Postal workers participate in bioterrorism response drill. Escorted by a police officer, a total of 2 million households in 5 cities will have a surprise visit from their letter carrier the summer of 2012, and they will deposit up to 2 bottles of emergency doxycyclene in each mailbox, first responders to a fictional anthrax, or other bioterrorist attack, the Washington Post reported July 12. Although the pill bottles will not actually contain real drugs, it is a scenario designed to prepare local officials for a biological terror attack with a quick strike delivered by the U.S. Postal Service. The mail carriers, all volunteers, are the lynchpin of a pilot program launched with a dry run May 6 in Minneapolis-St. Paul and will continue until the end of September in Louisville, Kentucky, San Diego, Boston, and Philadelphia. With a $10 million budget, the postal service is teaming up with the Department of Health and Human Services, State, and local health officials and law enforcement agencies to devise a program that would deliver antibiotics to thousands of households in each city within hours of an attack. Officials said the mail carriers could be deployed as soon as the Centers for Disease Control and Prevention gave the order to local health officials to release medicine. Source: http://www.salemnews.com/nationworld/x1447682109/Postal-workers-participate-in-bioterrorism-response-drill

(Wisconsin) **Man found guilty in post office threat.** A La Crosse, Wisconsin man charged with threatening to blow up the post office was found guilty July 10 after entering an insanity plea. A judge found him guilty on a felony charge of causing a bomb scare. On August 31, 2011, he demanded to speak to an Internal Revenue Service agent on the second-floor of the La Crosse post office before saying he would "blow this place up," according to the complaint. He fled the building and returned for a second time to a U.S. Representative's office yelling and demanding to see the Congressman, who was in the office, the complaint stated. One of the Congressman's staff members blocked the defendant from getting into the office and pushed him out the door.

The defendant then threatened they were all "gonners," according to the complaint. A disorderly conduct charge was dismissed but can be considered during his July 30 sentencing in La Crosse County Circuit Court. Source: http://lacrossetribune.com/news/man-found-guilty-in-post-office-threat/article_6de8653c-cb0e-11e1-a4b6-001a4bcf887a.html?comment_form=true

Public Health

FDA announces new safety plan for opioid use. The Food and Drug Administration (FDA) announced new safety measures for manufacturers and doctors who prescribe a class of opioid medication used to treat moderate to severe chronic pain. Opioids are powerful, but they can also cause serious harm, including overdose and death. "In 2008, nearly 15,000 Americans died where opioids were involved," said an FDA commissioner. "In 2009, that number went up to 16,000." To address the issue, the FDA provided a blueprint to more than 20 companies that manufacture opioid analgesics on how to educate physicians who prescribe them. The guidelines will include data on weighing the risks and benefits of opioid therapy, choosing patients appropriately, and managing, monitoring and counseling patients. The education will also include data on how to recognize evidence of opioid misuse, abuse, and addiction. Manufacturers will also have to provide an "easier to read" information sheet for patients. The FDA expects manufacturers to meet their obligations by giving educational grants to drug education providers, who will develop and deliver the training for physicians and heath care workers, as they do with other drugs. Source: http://thechart.blogs.cnn.com/2012/07/10/fda-announces-new-safety-plan-for-opioid-use/

(Florida) **Thousands feared exposed to Florida tuberculosis outbreak.** A stubborn and deadly outbreak of tuberculosis (TB) in Jacksonville, Florida, is prompting Florida to team up with the U.S. Centers for Disease Control and Prevention (CDC) to battle the disease, but State health officials insist the situation is under control. The TB outbreak is linked to 13 deaths and nearly 100 illnesses since 2004, mainly among homeless people. It is estimated about 3,000 people have been exposed to the contagious disease but that information was never released to the media. Now State and federal health workers are trying to track down as many of those people as possible to check for symptoms of TB, including cough, fever, sweats and weight loss. Florida asked the CDC for help with the TB cluster in February but not because the situation was out of control, according to a doctor with the State Department of Health. He called it business as usual. He said the cluster of TB cases did not warrant a public warning because it was not a public health hazard, and said Florida has the resources to reach out to those potentially exposed to tuberculosis with federal, State, and local governments contributing to the effort. The ongoing outbreak has coincided with the shutdown of Florida's only TB hospital — A.G. Holley in Lantana. The hospital closed the week of July 2 after State lawmakers passed and the Florida governor signed legislation eliminating funding for the facility. Source: http://www.wtsp.com/news/article/263133/12/Thousands-feared-exposed-to-Florida-tuberculosis-outbreak

U.S. allots $971 million in medical readiness aid. The Center for Infectious Disease Research and Policy reported that the U.S. Health and Human Services Department July 2 said it would

provide $971 million in medical readiness funding to States and jurisdictions. The amount includes $619 million for distribution under the Public Health Emergency Preparedness cooperative agreement, a marginal funding boost for the effort overseen by the U.S. Centers for Disease Control and Prevention. An additional $352 million is slated for distribution under the Hospital Preparedness Program, which aims to help States, territories, and local jurisdictions ready hospitals to handle an influx of patients following a planned or natural disease outbreak. The initiative received the same level of funding in 2011. Federal offices have been moving to improve coordination between the two funding initiatives, according to an HHS statement. Source: http://www.nti.org/gsn/article/us-disperse-971-million-medical-readiness-aid/

TRANSPORTATION

(Michigan) **Detroit-Windsor Tunnel reopens after bomb threat.** An international commuter tunnel connecting Detroit to Windsor, Ontario, was closed for nearly 4 hours July 12 after a bomb threat was phoned in on the Canadian side. No explosives were found, CBS News reported July 13. The Detroit Windsor Tunnel, a busy border crossing beneath the Detroit River, was shut down after a duty free shop employee on the tunnel's Canadian plaza reported receiving a call about a bomb threat. The tunnel was closed and traffic on both sides of the river was directed to the nearby Ambassador Bridge, which spans the river, the tunnel's executive vice president said. Homeland Security, U.S. Customs and Border Protection, Detroit police, and other agencies flooded the plaza and entrance on the tunnel's U.S. side. The bomb threat also resulted in heightened security along the Ambassador Bridge, west of downtown Detroit. The 82-year-old tunnel stretches about 1 mile across the Detroit River, which is one of North America's busiest trade crossings. Cars and buses make up most of the traffic. About 4.5 million cars crossed in 2011. After the call came in, officials at the tunnel followed protocol that is established between the tunnel operators and local emergency services officials in consultation with U.S. Customs and Border Protection, tunnel officials said. Source: http://www.cbsnews.com/8301-505245_162-57471753/detroit-windsor-tunnel-reopens-after-bomb-threat/

(Ohio) **Train crew was not speeding before derailment, investigators say.** Officials said July 12 that a train that derailed and exploded July 11 was not speeding, and that crew members saw nothing unusual on the track before the crash in Columbus, Ohio. According to the National Transportation Safety Board (NTSB), the Norfolk Southern train was traveling southbound from Chicago to Linwood, North Carolina, at 23 mph, and approaching a "fairly aggressive" curve in the track, and had a clear signal. Seventeen train cars derailed, there was an explosion, and four train cars carrying ethanol caught fire. The train, a little more than 1 mile long and with 2 locomotives and 98 freight cars was carrying 12,319 tons of material, including ethanol, styrene monomer, grain and corn syrup. At the time of the explosion, there were 90,000 gallons of ethanol on the train. Three ethanol cars and one car hauling wheat caught fire. Two people who were in the vicinity of the train when it derailed were injured. The victims drove themselves to the hospital. Residents in the area were evacuated after the crash. As of late afternoon July 12, officials said the four train cars that burned after the derailment remained at the site but clear

of the tracks. Norfolk Southern employees were working to repair the two lines of track, and there was no estimated time for when full train traffic would be restored. Source: http://www2.nbc4i.com/news/2012/jul/12/4/train-crew-was-not-speeding-derailment-investigato-ar-1100790/

(California) **FBI joins probe of explosives found under O.C. bridge.** The FBI was brought in to help investigate a cache of explosives — grenades, blasting caps and fuse igniters — that was found in a backpack under a bridge in Placentia, California, July 9. Orange County bomb squad officials were brought in after the backpack was discovered by people working in a drainage ditch, said an Orange County sheriff's spokesman. After cordoning off the area, bomb technicians detonated the contents of the backpack, including six grenades, blasting caps, fuse igniters, and blasting powder. For several hours, Lakeview Avenue between Orangethorpe Avenue and Eisenhower Circle was closed to traffic. "It was a dangerous situation," the spokesman said. "It could have caused major structural damage to the bridge." Source: http://latimesblogs.latimes.com/lanow/2012/07/officials-detonate-explosives-in-anaheim-.html

Water and Dams

Nothing Significant to Report

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168